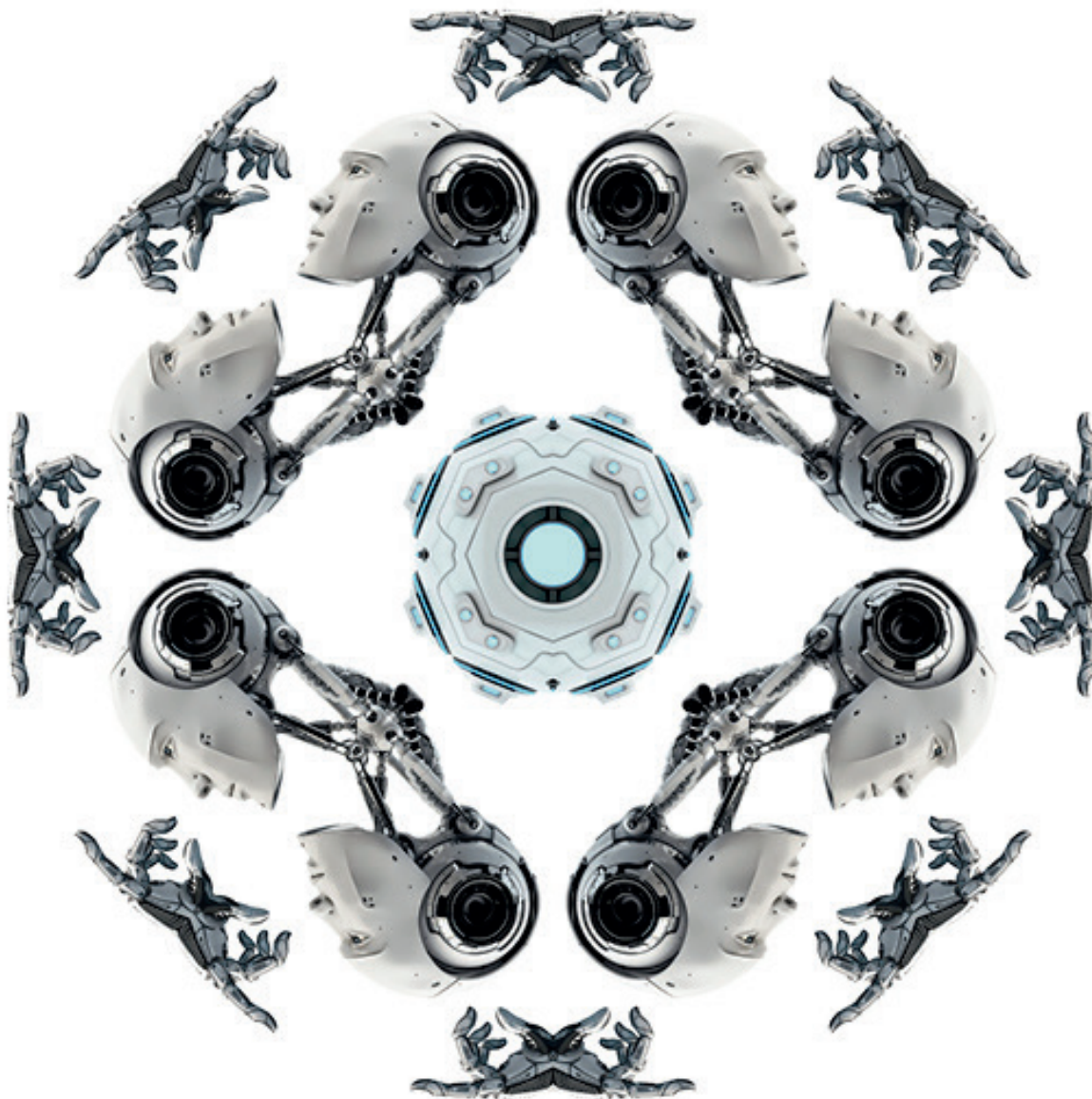




Inteligencia cibernética

¿Cómo puede la IA ayudar a manejar el riesgo cibernético?

Cyber





Manejo del riesgo cibernético con inteligencia cibernética

En la era digital, las tecnologías de inteligencia artificial empiezan a tener el mismo impacto revolucionario que las fábricas y las líneas de montaje tuvieron en la manufactura en los albores de la era industrial, al mejorar de forma dramática la eficiencia y habilitar nuevos productos, servicios y modelos de negocios que antes simplemente no eran posibles

Impulsadas por presiones internas y externas para evolucionar y madurar continuamente sus capacidades de mitigar y minimizar los riesgos cibernéticos, las organizaciones exploran intensamente nuevas tecnologías y oportunidades de mejora en todo lugar posible.

La inteligencia artificial (IA) está de moda en las salas de juntas directivas y en los pasillos, e impulsa la innovación a nuevos niveles en muchas áreas de los negocios. Los avances en tecnologías de IA, en capacidades de procesamiento y en disponibilidad de datos permiten que los sistemas informáticos realicen en la actualidad tareas que alguna vez requirieron de inteligencia humana para llevarse a cabo. Algunos ejemplos incluyen el aprendizaje automatizado, el procesamiento de lenguaje natural, el reconocimiento del habla, la visión por computadora, la comprensión de imágenes y la robótica.

En cibernética, las tecnologías de IA pueden mejorar la inteligencia de amenazas, la predicción y la protección. También pueden facilitar detección y respuestas más rápidas

ante ataques, al tiempo que reducen la necesidad de expertos humanos o especialistas en seguridad cibernética, tan escasos en estos días¹. La IA puede aprender de los analistas de seguridad y mejorar su desempeño paulatinamente conduciendo al ahorro de tiempo y a la toma de mejores decisiones. Estas capacidades en inteligencia se necesitan con urgencia, dado que los ciberataques aumentan en volumen y sofisticación.

La analítica y el big data son claves para facilitar la IA, pues permiten procesar y analizar vastas cantidades de datos (análisis, filtrado y visualización casi en tiempo real). La adopción de la analítica avanzada también es fundamental para convertirse en una organización guiada por el conocimiento.

Este informe describe cómo se pueden emplear las tecnologías de IA para mejorar las capacidades de ciberseguridad y manejar el riesgo cibernético de forma más eficiente y eficaz.

1. *Los rostros cambiantes de la seguridad cibernética: cerrando brechas de ciber riesgo*, Deloitte, 2018

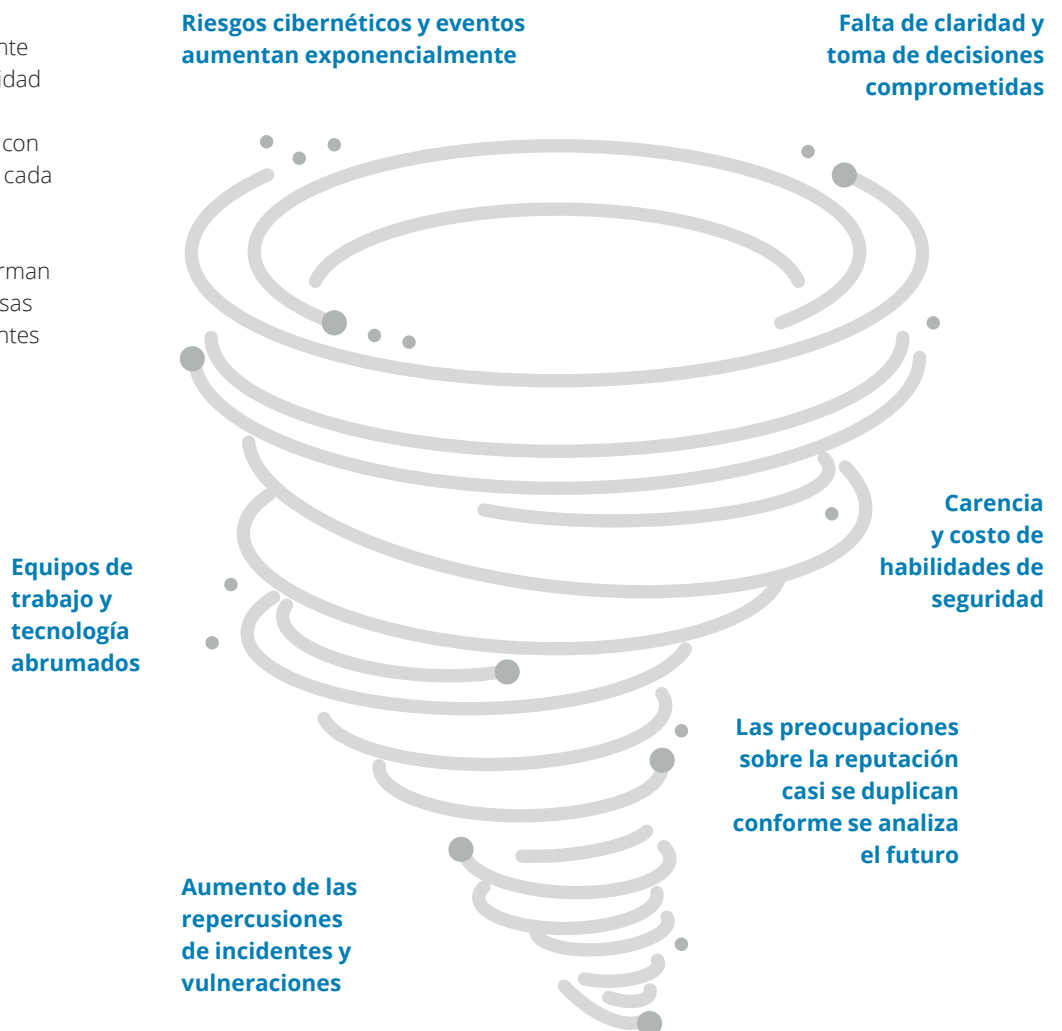
Una tormenta perfecta para el riesgo cibernético

La ciberseguridad es uno de los mayores desafíos de la era digital y crece día a día.

Las amenazas cibernéticas aumentan de forma exponencial. Las internas aprenden a evadir los sistemas basados en firmas, mientras que los actores malintencionados emplean IA para anticipar las reglas más comunes de detección y no ser descubiertos.

El tamaño y la complejidad de este latente desafío abruma a los equipos de seguridad cibernética, al tiempo que el talento calificado necesario para contraatacar con éxito los ataques en ciberseguridad, es cada vez más caro y difícil de encontrar.

Todas estas fuerzas combinadas conforman una tormenta perfecta. Pero las empresas pueden valerse de tecnologías emergentes para ayudarse a sobrellevar lo peor.



Las tecnologías cibernéticas inteligentes abarcan un amplio espectro, desde la automatización basada en reglas básicas que imita la acción humana, hasta la inteligencia artificial predictiva que imita, y hasta sobrepasa, la inteligencia y el juicio humanos. (Figura 1).

Figura 1: El espectro de las tecnologías cibernéticas inteligentes



El aprendizaje automatizado usa técnicas estadísticas y algoritmos que repetitivamente aprenden de datos y, automáticamente construye y mejora modelos sin programación adicional. Esto tiene numerosas aplicaciones potenciales en seguridad cibernética, como habilitar capacidades cibernéticas automatizadas y predictivas mediante las cuales un agente de *software* puede identificar un ataque activo y hacer los cambios necesarios para frustrarlo.

El procesamiento de lenguaje natural (NLP, por sus siglas en inglés) también tiene aplicaciones medulares en seguridad cibernética, incluyendo la prevención de fugas de datos. A partir de la analítica de comportamiento para crear marcadores de líneas base del comportamiento normal de los usuarios, el NLP podría desarrollar un perfil para cada usuario y luego supervisar acontecimientos atípicos mientras aprende e infiere continuamente de los nuevos patrones de comportamiento.

En el ámbito de la seguridad y el riesgo cibernéticos, las capacidades actuales son más maduras en la parte del espectro tecnológico que concierne a automatización de procesos robóticos (RPA, por sus siglas en inglés). Sin embargo, el objetivo más sofisticado (la inteligencia cognitiva y artificial) evoluciona rápidamente. Esto es impulsado por cinco factores principales:

- 1 Creciente precisión de los algoritmos predictivos**
Los avances en el aprendizaje automatizado mejoran la capacidad de la inteligencia predictiva de riesgo para identificar riesgos emergentes.
- 2 Disminución de costos de la tecnología**
A medida que las capacidades de automatización y computación se vuelven más rápidas y baratas, resulta más económico utilizar modelos predictivos de riesgo.
- 3 Creciente disponibilidad de fuentes de datos**
Junto con los avances en la analítica de datos no estructurados, la disponibilidad de bases de datos ricas, tanto externas como internas, aumenta el poder y el impacto de la inteligencia predictiva de riesgo.
- 4 Creciente sofisticación de las tecnologías de IA**
La IA ya tiene la capacidad de generar sus propias hipótesis (por ejemplo, predecir técnicas de ataque) y dar recomendaciones para abordarlas.
- 5 Manejo del riesgo para impulsar el valor comercial**
El riesgo es una parte integral de las empresas; sin embargo, conseguir la información predictiva para tomar decisiones más inteligentes puede ser una fuente valiosa de ventaja competitiva.

De acuerdo con el Laboratorio de Informática e Inteligencia Artificial del MIT, el futuro previsible de la seguridad cibernética probablemente girará en torno a un enfoque híbrido, con seres humanos y máquinas trabajando juntos para gestionar el riesgo cibernético de forma más eficaz y eficiente.

Ventajas de la inteligencia cibernética

Al aplicar IA y analítica a grandes cantidades de datos internos y externos, las tecnologías cibernéticas inteligentes pueden generar conocimientos predictivos que ayuden a tomar **mejores** decisiones cibernéticas y a proteger a las empresas de amenazas. También pueden ayudar a detectar y responder ante amenazas con **más rapidez** monitoreando el entorno cibernético con una velocidad y precisión que solo las máquinas pueden dar. Tal vez lo más importante es que la inteligencia cibernética ayuda a mantenerse al día frente al infinito bombardeo de ataques que son cada vez más sofisticados.

El tradicional enfoque escalonado de la seguridad cibernética sólo puede impedir y detectar las amenazas menos sofisticadas. Pero, mientras tanto, los ciberataques modernos son cuidadosamente diseñados para eludir los controles tradicionales de seguridad mediante el aprendizaje de las reglas de detección. Además, es posible que los controles tradicionales no aborden adecuadamente las amenazas internas, que son una forma traicionera de ataque de usuarios con accesos legítimos.

Cuando aprovechan inmensas fuentes de datos, las plataformas de detección inteligente pueden aprender y reconocer comportamientos normales, desarrollar líneas base y detectar los valores atípicos,

identificar las acciones maliciosas que se asemejan a eventos vistos anteriormente y hacer predicciones sobre otras amenazas nunca antes vistas. Estos objetivos no pueden alcanzarse con controles tradicionales basados en normas y firmas.

Además, las tecnologías cibernéticas inteligentes realizan tareas muy consistentes y de forma repetitiva, lo cual reduce la intervención manual y los errores humanos. Esto tiene el beneficio adicional de hacer más sencillo asegurar, gestionar y auditar el entorno cibernético, para lograr el **cumplimiento** de los reglamentos gubernamentales y otros requisitos externos.

Por último, pero no menos importante, las tecnologías cibernéticas inteligentes pueden ayudar a sacar el máximo provecho a los escasos **talentos** de ciberseguridad. Ellas permiten a los equipos cibernéticos hacer su trabajo con menos recursos, primero, al asumir el trabajo pesado de tareas rutinarias y que requieren mucha mano de obra, para que los expertos humanos se concentren en actividades que son más valiosas y estratégicas, y, segundo, al dar herramientas a los especialistas cibernéticos para que se desempeñen con alto nivel sin necesitar años de experiencia y formación.

Beneficios clave de las tecnologías cibernéticas inteligentes



- Complementan las aplicaciones y los controles de seguridad existentes con la detección de amenazas progresivas, emergentes y desconocidas.
- Facilitan a las empresas detectar amenazas avanzadas persistentes e identificar indicadores de compromiso que pueden no ser detectados con las defensas de seguridad existentes.
- Mejoran el proceso de búsqueda de amenazas mediante la recolección, la correlación y el análisis de una amplia gama de datos de seguridad.
- Determinan patrones de amenazas mediante fuentes de inteligencia de amenazas, información sobre vulnerabilidad, registros de eventos de dispositivos y datos contextuales, lo que permite una visión de seguridad proactiva y predictiva.

Anticipar riesgos con la inteligencia predictiva del riesgo

La gestión del riesgo cibernético ha sido una actividad típicamente reactiva, centrada en los riesgos y los eventos de pérdida que ya han ocurrido. Sin embargo, con la creciente adopción de tecnologías avanzadas de analítica e IA, la práctica cada vez se orienta más hacia el futuro y es más predictiva.

La inteligencia predictiva del riesgo utiliza IA y analítica para anticipar los riesgos emergentes, aumentar la conciencia de las amenazas externas y mejorar la comprensión empresarial de la exposición al riesgo y las pérdidas potenciales.

Las actividades de monitoreo ahora son parte del ciclo de vida de la gestión de riesgos y pueden dividirse en tres categorías:

Actividades reactivas

Capturan pérdidas e identifican los eventos pasados que casi fallan. Elaboran información de referencia para cuantificar el impacto de las pérdidas de los eventos. Informan sobre el estado de los riesgos actuales y las acciones correctivas.

Actividades predictivas

Acumulan e integran información interna y externa para generar alertas de información en tiempo casi real. Describen tendencias y riesgos emergentes. Utilizan insumos reactivos e integrados para generar información predictiva de riesgo con analítica avanzada.

Actividades integradas

Miden objetivamente el desempeño del riesgo facilitando la elaboración de indicadores clave de riesgo, indicadores clave de rendimiento y medidas límite asociadas. Posibilitan una descripción precisa de la exposición al riesgo aportando una visión holística en toda la empresa.

¿Cómo aplicar inteligencia predictiva del riesgo en su organización?

Este tipo de inteligencia de riesgo probablemente podría ayudar a su organización en cuatro áreas importantes de seguridad cibernética:

- **Toma de decisiones relacionadas con el riesgo.** Analizar grandes volúmenes de datos contextuales y puntos de decisión para determinar elecciones racionales y ayuda a los ejecutivos a tomar decisiones estratégicas y financieras alineadas con el apetito de riesgo de la organización (por ejemplo: analizar datos históricos de inversión y noticias financieras en tiempo real para tomar decisiones de inversión; evaluar y analizar racionalmente los riesgos patrimoniales).
- **Detección de riesgos.** Identificación o predicción de riesgos que son difíciles de detectar para los seres humanos y los sistemas basados en reglas, tales como nuevas categorías de riesgos, señales de riesgo difusas, o fuentes potenciales de riesgos futuros (por ejemplo, utilizando datos de foros públicos—como redes sociales y blogs—donde los clientes, críticos y otros grupos discuten y analizan la reputación de una organización y sus riesgos relacionados).
- **Monitoreo y detección de amenazas.** Monitoreo de las actividades y entidades para establecer un comportamiento normal y detectar anomalías que podrían crear riesgos (por ejemplo, detección de fraude y lavado de dinero; detección de amenazas infiltradas, incluidos los riesgos cibernéticos y de cumplimiento por parte de quienes tienen información privilegiada; inteligencia de amenazas cibernéticas en tiempo real).
- **Automatización de procesos de riesgo.** Automatización de procesos de riesgo complejos, que requieren gran cantidad de mano de obra y son propensos a errores, que manejen un alto volumen de datos estructurados y no estructurados (por ejemplo, la debida diligencia de terceros; gestión de identidad y acceso; gestión de riesgos crediticios; modelos de gestión de riesgo), especialmente los procesos que podrían beneficiarse de una herramienta que autoaprende con el tiempo.

¿Por dónde comenzar?

Muchas empresas se asientan sobre una multitud de datos valiosos que permanece enterrada bajo una maraña de procesos empresariales desconectados de ineficientes, por lo que es difícil saber dónde y cómo empezar. Para ayudar, Deloitte desarrolló un marco de trabajo basado en capacidades para identificar áreas específicas en las que se pueden aplicar tecnologías de IA y analítica cibernética. El marco se presenta como un cuadro que abarca todas las fases de la seguridad cibernética. (Figura 2).

Gobernanza

1 St Estrategia y modelo operativo		
2 Pa Políticas, estándares y arquitectura	5 Cs Seguridad en la nube	9 S Ciclo de vida de desarrollo de software seguro
3 Aw Riesgo cibernético y comportamiento	6 Tp Gestión del riesgo con terceros	10 Ap Protección de aplicaciones post desarrollo
4 Rm Gestión de riesgo cibernético, métricas y reporte	7 Hs Seguridad de recursos humanos	11 Mp Protección de malware
	8 Ps Seguridad física	12 Ns Seguridad de redes

● Gestión de seguridad cibernética

- Empresa extendida
- Personas y lugar de trabajo

● Seguridad de la aplicación

Figura 2: La tabla periódica de los elementos de seguridad cibernética

1	Número de la capacidad
St	Símbolo
Estrategia y modelo operativo	Nombre de la capacidad

Resiliente

32
Ip
Preparación para incidentes

33
Ir
Respuesta a incidentes

34
Bc
Gestión de la continuidad del negocio y la resiliencia

● Gestión de incidencias
● Resiliencia empresarial

Seguro

Vigilante

13
Es
Seguridad de dispositivos de usuario final

17
Idm
Gestión del ciclo de vida de identidad

21
Dlp
Prevención de pérdida de datos

25
Cti
Inteligencia de amenazas cibernéticas

29
Sp
Administración de la plataforma de seguridad

14
Am
Administración de activos

18
Pam
Gestión de acceso privilegiado

22
E
Encriptación

26
Bp
Protección de marcas

30
Pvm
Gestión de vulnerabilidad y parches

15
Ss
Seguridad del sistema

19
Rbac
Control de acceso basado en roles

23
Dp
Privacidad de datos

27
Td
Detección de amenazas

31
Pvi
Pruebas de penetración e identificación de vulnerabilidades

16
Ua
Control de acceso de usuarios

20
Ic
Clasificación de información

24
Ilm
Gestión del ciclo de vida de la información

28
Th
Caza de amenazas

● Identificación de vulnerabilidad

● Seguridad de infraestructura

● Gestión de identidad y acceso

● Seguridad de datos

● Inteligencia de amenazas

● Operaciones de seguridad

Los siguientes son algunos casos cautivadores para **automatización** en áreas específicas de seguridad cibernética, que pueden incluir múltiples elementos en el cuadro.

4	Rm Gestión de riesgo cibernético, métricas y reporte	Gobernanza, riesgo y cumplimiento La gobernanza y la gestión de riesgos Informan de la estrategia general y mejoran las capacidades de presentación de informes utilizando grandes volúmenes de datos contextuales y puntos decisivos para ayudar a tomar decisiones estratégicas ajustadas al apetito por el riesgo de la organización. Síntesis y mapeo de reglamentos Desarrolla y mantiene el marco de control de seguridad integrado de una organización, extrayendo información de múltiples fuentes reglamentarias y directrices. Evaluaciones desencadenantes Realiza evaluaciones automatizadas periódicamente, o se activan periódicamente por cambios en las aplicaciones y/o procesos de negocio. Automatización de indicadores claves de riesgo Automatiza la recolección y visualización de indicadores clave de riesgo para facilitar a la empresa evaluar y abordar la exposición al riesgo. Asignación de responsabilidades Emplea procesos de autoservicio para asignar responsabilidades de seguridad cibernética entre los equipos, mejorando la eficiencia y permitiendo una mayor alienación con los propietarios del riesgo. Pruebas de control Automatiza las pruebas de control para que evalúen continuamente la efectividad del control y proporcione actualizaciones casi en tiempo real sobre la postura de seguridad de la organización.	17	Idm Gestión del ciclo de vida de identidad	Gestión de identidad y acceso (IAM) Mantenimiento de roles Emplea un motor de IA para ofrecer recomendaciones sobre el mantenimiento de roles, ayudando a las organizaciones a racionalizar la difícil costosa y larga tarea de mantener al día las definiciones de los roles. Motor de minería de roles Extiende el motor de mantenimiento de roles desde múltiples fuentes de datos, recomendando nuevos roles y derechos. Motor de recomendación de solicitud de acceso Simplifica el proceso de solicitud de acceso analizando varias fuentes de datos (tales como el acceso de pares de grupo y las solicitudes de acceso histórico) y luego recomienda el nivel requerido para un usuario. Analítica del acceso a la certificación Analiza diferentes bases de datos y aplica analítica para mejorar el proceso de certificación mediante: la preaprobación de los elementos de certificación basados en los datos de solicitud de acceso, la detección de anomalías en el ciclo de la certificación y el uso de datos de grupo para calcular un puntaje de confianza que ayude a los revisores a tomar decisiones informadas. Datos de uso de acceso para el motor de analítica Incorpora los datos de uso de acceso en el motor de analítica para ayudarle a generar insumos más informados y eficientes.
			18	Pam Gestión de acceso privilegiado	

En el extremo más sofisticado del espectro tecnológico, los siguientes son algunos de los muchos usos potenciales para las **tecnologías de IA y analítica** en seguridad cibernética.

15

Ss

Seguridad del sistema

Seguridad del sistema

Eficacia del control

Aumenta y evalúa la eficacia de las herramientas probadas tales como firewalls, proxies y soluciones de prevención de pérdidas de datos mediante el monitoreo de los datos de registro disponibles y luego identificando y reparando errores de configuración.

25

Cti

Inteligencia de amenazas cibernéticas

Inteligencia de amenazas cibernéticas

Detección de los riesgos cibernéticos

Identifica o predice riesgos que a menudo son difíciles de detectar para los seres humanos y los sistemas basados en reglas, incluyendo nuevas categorías de riesgos, señales de riesgo difusas y fuentes potenciales de riesgos futuros, como un creciente uso de las redes sociales.

27

Td

Detección de amenazas

Detección de amenazas

Detección de comportamientos atípicos

Ayuda a identificar la actividad atípica de acceso a datos y la actividad maliciosa de la aplicación se centra en los inicios de sesión de los usuarios, los cambios en el comportamiento de los usuarios y cambios no aprobados.

Descubrimiento de amenazas

Monitorea las actividades y entidades para establecer un comportamiento normal y detectar fuentes de anomalías que podrían crear riesgos potenciales como el fraude, el lavado de dinero y las amenazas infiltradas.

Limpieza de alertas y priorización

Emplea el aprendizaje automatizado para automatizar significativamente el primer nivel de clasificación basado en factores como tipo de ataque, frecuencia y experiencia previa.

Investigación y apoyo selectivos

Emplea una plataforma de big data para impulsar nuevos conocimientos a través del análisis histórico, permitiendo así que las investigaciones de incidentes basados en datos actuales e históricos se hagan de forma rápida y eficiente.

28

Th

Caza de amenazas

Caza de amenazas y gestión de la vulnerabilidad

Caza de amenazas

Busca rápidamente nuevas amenazas importando tácticas, técnicas, procedimientos y patrones de ataque conocidos (junto con detalles de vulnerabilidad e información remedial) para ayudar a neutralizar amenazas al inicio del ciclo de ataque.

Escaneo de vulnerabilidad

Emplea bots para iniciar y escanear aplicaciones, sistemas y otros activos de vulnerabilidades, evaluando el riesgo y priorizando el programa de parches.

Revisión de configuración

Utiliza los bots para revisar las configuraciones del sistema y asegurar el endurecimiento de la línea base y que no haya errores en las configuraciones.

Modelado de trayectoria de ataque

Realiza analítica predictiva sobre los datos de seguridad para determinar puntos de entrada vulnerables y el camino probable que un atacante podría utilizar para acceder.

30

Pvm

Gestión de vulnerabilidad y parches

De la promesa a la práctica

Las tecnologías de la inteligencia artificial han estado recibiendo mucha atención últimamente. Ahora es el momento de pasar de hablar a la acción. Aquí hay siete pasos que puede empezar a dar ya para aumentar las capacidades cibernéticas de su organización a través del uso de tecnologías de IA y analítica.



1

Acepte el futuro

Colabore con su ecosistema para ayudar a modelar el futuro de estas nuevas y poderosas tecnologías cibernéticas.

2

Edúquese a sí mismo y a sus equipos

Conozca las oportunidades de negocio asociadas con las tecnologías de IA y analítica en cibernética, sumérjase en foros internos y procesos de toma de decisiones para ser un contribuyente valioso.

3

Reconsidere el panorama de riesgos y amenazas

Comprenda el impacto de las nuevas tecnologías y desarrolle respuestas adecuadas de gestión de riesgos.

4

Redefina su modelo de rendición de cuentas

Considere cómo los cambios en el ambiente operacional afectarán el panorama de riesgos y los controles necesarios y luego ajuste consecuentemente los roles y responsabilidades de su equipo cibernético.

5

Racionalice su marco de control

Fomente el diseño inteligente para los riesgos de los nuevos sistemas, tecnologías y marcos de control, para reducir las capas de control innecesarias y construir más capacidades preventivas y automatizadas al principio.

6

Inicie pequeño y escale rápido

Desarrolle una estrategia rápida para aplicar las tecnologías y analítica de AI a la seguridad cibernética mediante la identificación de oportunidades con alto impacto, baja complejidad, datos fácilmente disponibles y capacidades actuales insuficientes.

7

Reconsidere su estrategia de talento cibernético

Actualice su estrategia de talento, dando pasos para asegurar que los profesionales cibernéticos altamente calificados lideren el camino en sus esfuerzos de seguridad cibernética.

Las tecnologías de AI y analítica pueden elevar las capacidades cibernéticas de su empresa al siguiente nivel. Al tomar la iniciativa en la aplicación de estas innovaciones disruptivas a la seguridad cibernética, puede inclinar la balanza a su favor y mantenerse un paso adelante de las amenazas.

Contactos

Autores



Nick Galletto

Líder Global y Canadá de
Ciberriesgo
ngalletto@deloitte.ca
+1 416 6016 734



Dina Kamal

Socio, Deloitte Canadá
Inteligencia Artificial
dkamal@deloitte.ca
+1 416 775 7414



Marc Mackinnon

Socio, Deloitte Canadá
Risk Advisory
mmackinnon@deloitte.ca
+1 416 601 5993

Líderes Regionales de Cibernética



Andrés Casas

Líder de Riesgo Cibernético de
Centroamérica y República Dominicana
ancasas@deloitte.com
+506 2246 5000



Andres Gil

Líder de Riesgo Cibernético de las
Américas
angil@deloitte.com
+54 114 390 2600



Chris Verdonck

Líder de Riesgo Cibernético de
EMEA
cverdonck@deloitte.com
+32 280 024 20



James NunnPrice

Líder de Riesgo Cibernético de
Asia Pacífico
jamesnunnprice@deloitte.com.au
+61 293 227 971





Deloitte se refiere a uno o más de Deloitte Touche Tohmatsu Limited ("DTTL"), su red global de firmas miembro y sus entidades relacionadas. DTTL (también conocido como "Deloitte Global") y cada una de sus firmas miembro son entidades legalmente separadas e independientes. DTTL no proporciona servicios a los clientes. Visite www.deloitte.com/about para obtener más información.

Deloitte es un proveedor global líder de auditoría y aseguramiento, consultoría, asesoría financiera, consultoría en riesgos, impuestos y servicios relacionados. Nuestra red de firmas miembro en más de 150 países y territorios atiende a cuatro de cada cinco compañías Fortune Global 500®. Conozca cómo las aproximadamente 286,000 personas de Deloitte tienen un impacto que importa en www.deloitte.com.

Esta comunicación solo contiene información general y nadie de Deloitte Touche Tohmatsu Limited, sus firmas miembro o sus entidades relacionadas (colectivamente, la "red de Deloitte"), a través de esta comunicación, presta asesoría o servicios profesionales. Antes de tomar una decisión o tomar alguna medida que pueda afectar sus finanzas o su negocio, debe consultar a un asesor profesional calificado. Ninguna entidad en la red de Deloitte será responsable por cualquier pérdida sufrida por cualquier persona que confíe en esta comunicación.